Shorewall pour OpenVPN

De Docs du CCRI

Sommaire

Installation de Shorewall

```
apt-get install shorewall
```

Configurer Shorewall

Le fichier de configuration shorewall.conf

Le fichier de configuration de shorewall **/etc/shorewall/shorewall.conf** n'a pas vocation à être souvent modifié.
Nous allons modifier tout de même certains paramètres :

```
IP_FORWARDING=On        # Sur certaines versions, cette option peut être à 'Off', ce qui empêche le NAT
```

Les logs

Par défaut, shorewall utilise les logs de netfilter.
Lorsque l'on décide d'activer les logs, tout va dans **/var/log/messages**.

Nous allons configurer shorewall et rediriger tous les logs vers un fichier spécifique.

```
apt-get install ulogd2
```

Nous allons modifier la configuration d'ulogd2, en modifiant le fichier de configuration **/etc/ulogd.conf**

```
[emu1]
file="/var/log/shorewall/shorewall.log"
sync=1
```

Créez le répertoire et les fichiers

```
mkdir /var/log/shorewall/
mv /var/log/shorewall-init.log /var/log/shorewall/
touch /var/log/shorewall/shorewall.log
```

Important : Dans toutes vos règles, il faudra utiliser le mot clef **NFLOG** pour rediriger les logs dans les bons fichiers.

Redémarrez ulogd

```
/etc/init.d/ulogd2 restart
```

Éditez **/etc/shorewall/shorewall.conf**

```
LOGFILE=/var/log/shorewall/shorewall.log
STARTUP_LOG=/var/log/shorewall/shorewall-init.log
```

Redémarrez shorewall

```
/etc/init.d/shorewall restart
```

Voici un récapitulatif des fichiers de logs :

```
/var/log/shorewall-init.log   # Ce fichier est rempli au démarrage ou redémarrage de shorewall.
/var/log/shorewall.log        # Ce fichier contient toutes les nouvelles connexions (autorisées, refusée
```

Important : Nous ne journalisons que les nouvelles connexions, dans un souci d'économie des ressources.

Rotation des logs

Il est important de garder les journaux du pare-feu : il faut penser à la rotation des logs.

Créez le fichier **/etc/logrotate.d/shorewall**

```
/var/log/shorewall/shorewall-init.log {
    weekly
    rotate 4
    compress
    missingok
    create 0640 root adm
}
```

```
/var/log/shorewall/shorewall.log {
    daily
    rotate 365
    compress
    missingok
    create 0666 root adm
    postrotate
        /etc/init.d/ulogd2 restart 2>/dev/null
    endscript
}
```

Les fichiers journalisés sont recréés tous les jours à 6H25.

Autoriser le démarrage de shorewall au démarrage du serveur

Éditez le fichier **/etc/default/shorewall**

```
startup=0
```

Mettez cette valeur à **1**

```
startup=1
```

Les zones

```
###############################################################################
#ZONE           TYPE    OPTIONS                 IN                      OUT
#                                       OPTIONS                 OPTIONS
fw              firewall
net             ipv4
```

```
vpn             ipv4
srv:net         ipv4
ccri:net        ipv4
```

Important : La zone **srv** est une sous-zone de la zone **net**.
La zone **ccri** est une sous-zone de la zone **net**.

Les interfaces

```
###############################################################################
?FORMAT 2
###############################################################################
#ZONE   INTERFACE       OPTIONS
net      eth0            tcpflags,routefilter,logmartians,nosmurfs
vpn      tun0            tcpflags,routefilter,logmartians,nosmurfs
```

Les règles appliquées par défaut (policy)

```
###############################################################################
#SOURCE         DEST            POLICY          LOG LEVEL       LIMIT:BURST
$FW             all             ACCEPT          NFLOG
net             $FW             DROP            NFLOG
net             all             DROP            NFLOG
# The FOLLOWING POLICY MUST BE LAST
all             all             REJECT          NFLOG
```

Le fichier hosts

```
#ZONE   HOSTS                   OPTIONS
srv     eth0:192.70.36.0/24     -
ccri    eth0:172.18.0.0/24      -
```

Important : Ce fichier sert à délimiter la zone **srv** à notre plage IP publique.

Le fichier des règles (rules)

```
# Shorewall version 4.0 - Sample Rules File for one-interface configuration.
# Copyright (C) 2006-2014 by the Shorewall Team
#
# This library is free software; you can redistribute it and/or
# modify it under the terms of the GNU Lesser General Public
# License as published by the Free Software Foundation; either
# version 2.1 of the License, or (at your option) any later version.
#
# See the file README.txt for further details.
#------------------------------------------------------------------------------------------------------------------
# For information on entries in this file, type "man shorewall-rules"
###################################################################################################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE          ORIGINAL        RATE
#                                                       PORT    PORT(S)         DEST            LIMIT
#
```

```
?SECTION NEW

# Drop packets in the INVALID state

Invalid(DROP)  net              $FW             tcp
###############################################################################################################
#  Accès au firewall
###############################################################################################################

# Accès SSH
SSH-IUT(ACCEPT):NFLOG   srv:192.70.36.0/24      $FW:192.70.36.52                                # Autori
SSH-IUT(ACCEPT):NFLOG   ccri:172.18.0.0/24      $FW:192.70.36.52                                # Autori

# Accès OpenVPN (Port HTTPS 443)
VPN-IUT(ACCEPT):NFLOG   net                     $FW:192.70.36.52                                # Autori

# Bacula serveur
BACULA-SRV(ACCEPT):NFLOG srv:192.70.36.22       $FW:192.70.36.52                                # Autori

# Ping
Ping(DROP):NFLOG        net                     $FW                                             # Bloque

# Ping
Ping(ACCEPT):NFLOG      srv:192.70.36.0/24      $FW:192.70.36.52                                # Autori
Ping(ACCEPT):NFLOG      vpn                     $FW:10.42.0.1                                   # Autori

###############################################################################################################
#                       VPN : CCRI                                                              #
###############################################################################################################

# Client : Benoît Tonnerre - benoit.tonnerre :          10.42.0.10
KMS(ACCEPT):NFLOG       vpn:10.42.0.10  net                                                     # Autori
HTTPS(ACCEPT):NFLOG     vpn:10.42.0.10  srv:192.70.36.55                                       # Autori
LDAP(ACCEPT):NFLOG      vpn:10.42.0.10  srv:192.70.36.33                                       # Autori
LDAP(ACCEPT):NFLOG      vpn:10.42.0.10  srv:192.70.36.27                                       # Autori
LDAPS(ACCEPT):NFLOG     vpn:10.42.0.10  srv:192.70.36.27                                       # Autori
SSH-IUT(ACCEPT):NFLOG   vpn:10.42.0.10  srv:192.70.36.33                                       # Autori
SMB(ACCEPT):NFLOG       vpn:10.42.0.10  srv:192.70.36.6                                        # Autori
HTTPS(ACCEPT):NFLOG     vpn:10.42.0.10  net:129.175.248.34                                     # Autori
MYSQL(ACCEPT):NFLOG     vpn:10.42.0.10  net:129.175.248.34                                     # Autori

# Client : Sébastien Gaudin - sebastien.gaudin :        10.42.0.11
HTTPS(ACCEPT):NFLOG     vpn:10.42.0.11  srv:192.70.36.55                                       # Autori

# Client : Éric Charron - eric.charron1 :               10.42.0.12

# Client : Nicolas Roux - nicolas.roux :                10.42.0.13

# Client : Olivier Guilleminot - olivier.guilleminot :  10.42.0.14

# Client : Joël Serre - joel.serre :                    10.42.0.15

###############################################################################################################
#                       VPN : Enseignants                                                       #
###############################################################################################################

# Client : Gaëlle Primault - gaelle.primault :          10.42.0.20

# Client : Marie-Pierre Morand - marie-pierre.morand :  10.42.0.21

# Client : Lydie Amann - lydie.amann :                  10.42.0.22

# Client : Grégoire Michelutti - gregoire.michelutti :  10.42.0.23

# Client : Sabine Marduel - sabine.marduel :            10.42.0.24
```

```
# Client : Claude Frappart - claude.frappart :          10.42.0.25
# Client : François Pesty - francois.pesty :            10.42.0.26
# Client : Maximilien Lagron - maximilien.lagron :      10.42.0.27
# Client : Élodie Leducq - elodie.leducq :              10.42.0.28
# Client : Odile Guiot - odile.guiot :                  10.42.0.29
# Client : Émmanuel Motchane - emmanuel.motchane :      10.42.0.30
# Client : Bruno Darracq - bruno.darracq :              10.42.0.31
# Client : Sergio Rodriguez - sergio.rodriguez :        10.42.0.32
# Client : Sylvie Drouin - sylvie.drouin :              10.42.0.33
# Client : Gilles Laschon - gilles.laschon :            10.42.0.34
# Client : Pascal Aubert - pascal.aubert :              10.42.0.35
```
